PATENT ABSTRACTS OF JAPAN

A9

(11)Publication number : 2002-204228
(43)Date of publication of application : 19.07.2002

(51)Int.Cl. H04L 9/08
G06F 15/00
H04L 9/14

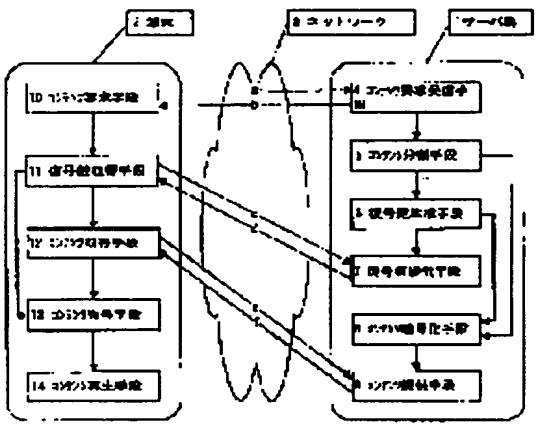
(21)Application number : 2000-400839
(22)Date of filing : 28.12.2000

(71)Applicant : HAYASHI TOSHINORI
YAMADA YASUHIKO
KYO SENMEI
NAKAHARA YORIJI

(72)Inventor : HAYASHI TOSHINORI
YAMADA YASUHIKO
KYO SENMEI
NAKAHARA YORIJI

(54) DEVICE AND METHOD FOR DISTRIBUTING CONTENTS, AND PROGRAM AND DEVICE FOR DOWNLOADING CONTENTS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a device for distribution of digital contents which enable prevention of illegal duplication and circulation of digital contents without spoiling the convenience for a legitimate user.
SOLUTION: The digital contents stored on a server are divided into two or more parts, which are each ciphered with different cipher keys and distributed to the user in the ciphered state and the cipher keys applicable to the distributed divided digital contents are distributed to the user.



LEGAL STATUS

[Date of request for examination] 30.01.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision

of rejection]
[Date of extinction of right]

Japanese Publication for Unexamined Patent Application

No. 2002-204228/2002 (Tokukai 2002-204228)

A. Relevance of the above-identified Document

The following is a partial English translation of exemplary portions of non-English language information that may be relevant to the issue of patentability of the claims of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

[DETAILED DESCRIPTION OF THE INVENTION]

[MEANS TO SOLVE THE PBOBLEMS]

[0007]

More specifically, the present invention is to provide a digital content delivering method for delivering digital content to a user, the digital content stored in a server. The method is characterized in that the digital content is divided in two or more portions, which are encrypted with different encryption keys respectively; the encrypted portions of the digital content are delivered to the user; and decoding keys applicable to the portions of the digital content are delivered to the user. This method is characterized in that, for the encrypted and delivered portions of the content, the entire content is delivered by user repeating (i) the step of receiving transmission of

THIS PAGE BLANK (USPTO)

a portion of the content, (ii) the step of acquiring via a network, a decoding key at the same time when the user receives the transmission of the portion of the content, the decoding key corresponding to the encryption key, (iii) the step of decoding the portion of the content by using the decoding key, and (iv) deleting the portion of content and the decoding key.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－204228
（P2002－204228A）
(43)公開日　平成14年７月19日(2002.7.19)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/00	３３０Ｚ　５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６０１Ｂ　５Ｊ１０４
Ｈ０４Ｌ　9/14			６４１

審査請求　未請求　請求項の数12　ＯＬ　（全　６　頁）

(21)出願番号　特願2000－400839(P2000－400839)

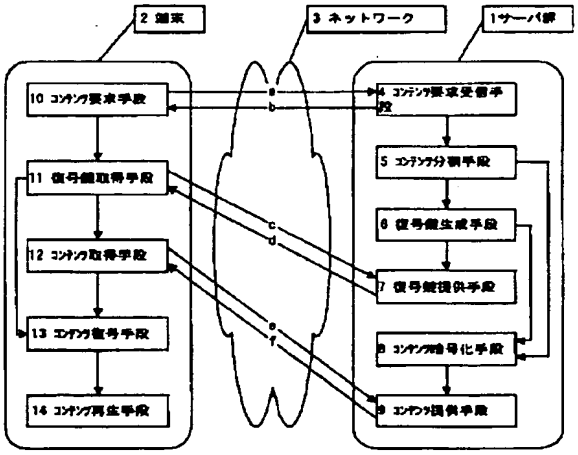
(22)出願日　平成12年12月28日(2000.12.28)

(71)出願人　501005036
林　利憲
北海道札幌市豊平区平岸１条６丁目３－56
(71)出願人　501005070
山田　康彦
東京都豊島区東池袋４丁目21－５
(71)出願人　501005117
許　先明
埼玉県所沢市寿町20－12
(74)代理人　100101982
弁理士　久米川　正光　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツ配信装置、コンテンツ配信方法、コンテンツダウンロードプログラム、コンテンツダウンロード装置

(57)【要約】
【課題】デジタルコンテンツ配信において、正当なユーザの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる配信方法や配信装置を提供することを目的とする。
【解決手段】サーバに蓄積されたデジタルコンテンツを二つ以上の部分に分割するとともに、そのそれぞれについて異なる暗号鍵によって暗号化し、分割されたデジタルコンテンツを暗号化した状態でユーザに配信するとともに、配信した分割デジタルコンテンツに適用可能な復号鍵をユーザに配信することを特徴とする、デジタルコンテンツ配信方法。



1

【特許請求の範囲】
【請求項１】デジタルコンテンツをネットワークを介して送信するためのコンテンツ配信装置であって、
ユーザからのコンテンツ要求を受信する要求受信手段と、
要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割手段と、
異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信する提供手段と、を含む、コンテンツ配信装置。
【請求項２】前記コンテンツ部分のそれぞれに対応する暗号鍵と複合鍵を生成する鍵生成手段を含む、請求項１のコンテンツ配信装置。
【請求項３】前記鍵生成手段によって生成した復号鍵をユーザに対して送信する鍵提供手段を含む、請求項１又は請求項２のコンテンツ配信装置。
【請求項４】前記鍵生成手段によって生成した暗号鍵によって、前記コンテンツ部分のそれぞれを暗号化する暗号化手段を含む、請求項１乃至請求項３のコンテンツ配信装置。
【請求項５】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、
ユーザからのコンテンツ要求を受信する要求受信ステップと、
要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、
異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、を含む、コンテンツ配信方法。
【請求項６】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、
ユーザからのコンテンツ要求を受信する要求受信ステップと、
要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、
前記コンテンツ部分のそれぞれに対応する暗号鍵を生成するステップと、
異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、を含む、コンテンツ配信方法。
【請求項７】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、
ユーザからのコンテンツ要求を受信する要求受信ステップと、
要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、
前記コンテンツ部分のそれぞれに対応する暗号鍵と復号鍵を生成するステップと、
異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、

2

前記部分コンテンツ毎の復号鍵をユーザに対して送信する復号鍵送信ステップと、を含む、コンテンツ配信方法。
【請求項８】サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロードプログラムであって、
暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する手段と、
前記部分コンテンツを復号する復号鍵を受信する手段と、
前記部分コンテンツに対し、前記復号鍵を適用する手段と、を含む、コンテンツダウンロードプログラム。
【請求項９】請求項８に係るコンテンツダウンロードプログラムを格納したコンテンツダウンロードプログラム記録媒体。
【請求項１０】サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロード装置であって、
暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する手段と、
前記部分コンテンツを復号する復号鍵を受信する手段と、
前記部分コンテンツに対し、前記復号鍵を適用する手段と、を含む、コンテンツダウンロード装置。
【請求項１１】サーバに蓄積されたデジタルコンテンツをユーザに配信する方法であって、
前記デジタルコンテンツを二つ以上の部分に分割するとともに、そのそれぞれについて異なる暗号鍵によって暗号化し、分割された前記デジタルコンテンツを暗号化した状態でユーザに配信するとともに、配信した前記分割されたデジタルコンテンツに適用可能な復号鍵をユーザに配信することを特徴とする、デジタルコンテンツ配信方法。
【請求項１２】サーバに蓄積されたデジタルコンテンツを受信する方法であって、
二つ以上の部分に分割された前記デジタルコンテンツの一部であり、独自の暗号鍵で暗号化された分割コンテンツを受信するとともに、前記分割コンテンツに適用可能な復号鍵を受信し、前記分割コンテンツに前記復号鍵を適用することを特徴とする、デジタルコンテンツ受信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルコンテンツをネットワーク上で販売する際に好適な著作権保護手法に関するものである。本発明は、特に、デジタルコンテンツをネットワーク上で販売する際のコンテンツ配信の際に、必要な不正アクセス防止手法に係るものである。
【０００２】

【従来の技術】デジタルコンテンツをネットワーク上で取引する際にコンテンツの著作権を保護する方法として、コンテンツを暗号化しその再生に専用の解読ソフトを用い、解読の際に特定のパスワード等の鍵情報を用いる方法（例えば、音楽配信に使用されるＳＤＭＩ(Secure Digital Music Initiative)規格と呼ばれる手法や世の中で有料放送で行われているスクランブル放送の手法が知られている）や、解読の際に所定の情報鍵をネットワーク上の鍵センタより取得し当該鍵を用いてコンテンツの復号・再生を行う方法等が考えられる。

【０００３】前者の方法では、コンテンツの不正な流通、利用を完全に防止できず、またコンテンツの正当なユーザの利便性をも損なうという問題があった。例えば、コンテンツをユーザ毎の暗号鍵を用いて、コンテンツを暗号化した上でデータを圧縮し、これをネットワークを介してユーザ側の端末に配送し、同時にダウンロードした対となる解読用の復合鍵を用いて、専用プレーヤー又はソフトウェアを用いて再生するという方法がこの方法の典型的な運用方法である。しかし、この方法では、特定の専用プレーヤー又はソフトウエアを用いることが復号の条件なので、専用プレーヤー又はソフトウエアが利用できない環境下（例えば、自宅以外の場所など）においては、著作権の利用権限を有する正当なユーザであっても、使用する端末（プレーヤも含めて）によっては再生が不可能になる等、コンテンツユーザの利便性を損なうという問題があった。

【０００４】後者の方法は、情報鍵を鍵センタより取得するため、特定の端末でないとコンテンツが利用できないという問題は解消され、ユーザの利便性を損なうことはない。しかし、所定の鍵を用いるため、鍵自体が不正にアクセスされて、流出したときには、コンテンツの不正な流通、利用を完全に防止できない。

【０００５】

【発明が解決しようとする課題】そこで、本発明は、デジタルコンテンツの配信において、正当なユーザの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる配信方法や配信装置を提供することを目的とするものである。

【０００６】

【課題を解決するための手段】前記課題を解決するため、本発明では、配信時にサーバ群上のコンテンツを任意の単位として分割することを特徴とする、デジタルコンテンツをネットワークに接続されたユーザの端末上で再生可能とするコンテンツの配信方法を提供する。

【０００７】より具体的にいうと、本発明は、サーバに蓄積されたデジタルコンテンツをユーザに配信する方法であって、デジタルコンテンツを二つ以上の部分に分割するとともに、そのそれぞれについて異なる暗号鍵によって暗号化し、分割されたデジタルコンテンツを暗号化した状態でユーザに配信するとともに、配信した分割デジタルコンテンツに適用可能な復号鍵をユーザに配信することを特徴とする、デジタルコンテンツ配信方法を提供するものである。このような方法で分割・暗号化・配信されたコンテンツについて、ユーザは分割コンテンツを受信するステップと、分割コンテンツを受信すると同時に前記暗号鍵に対応する復号鍵をネットワークを通じて取得するステップと、前記復号鍵を用いて前記分割コンテンツを復号するステップと、前記分割コンテンツと前記復号鍵を削除するステップを繰り返すことによって、コンテンツ全体の配信を行うことを特徴とする。

【０００８】より具体的にいうと、ユーザについては、本発明は、サーバに蓄積されたデジタルコンテンツを受信する方法であって、二つ以上の部分に分割された前記デジタルコンテンツの一部であり、独自の暗号鍵で暗号化された分割コンテンツを受信するとともに、分割コンテンツに適用可能な復号鍵を受信し、分割コンテンツに前記復号鍵を適用することを特徴とする、デジタルコンテンツ受信方法として説明することができる。

【０００９】本発明に係る解決手段をさらに説明すると、例えば、以下のようになる。即ち、本発明は、デジタルコンテンツをネットワークを介して送信するためのコンテンツ配信装置であって、ユーザからのコンテンツ要求を受信する機構と、要求されたコンテンツを二つ以上のコンテンツ部分に分割する機構と、異なる暗号鍵で暗号化されたコンテンツ部分をユーザに対して送信する機構と、を含むものである。

【００１０】本発明は、さらに、コンテンツ部分のそれぞれに対応する暗号鍵と複合鍵を生成する鍵生成機構、鍵生成手段によって生成した復号鍵をユーザに対して送信する鍵提供機構、鍵生成手段によって生成した暗号鍵によって、コンテンツ部分のそれぞれを暗号化する暗号化機構のいずれか一つ又は二つ以上を含むものであっても構わない。

【００１１】また、本発明は、デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、ユーザからのコンテンツ要求を受信する要求受信ステップと、要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、を含むものである。このコンテンツ配信方法は、コンテンツ部分のそれぞれに対応する暗号鍵を生成するステップ、若しくは、コンテンツ部分のそれぞれに対応する暗号鍵及び復号鍵を生成するステップを含むものであっても構わない。

【００１２】また、本発明をユーザの使用するプログラムという形で示すと以下のようになる。即ち、本発明は、サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロードプログラムであって、暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する機構と、部分コンテンツを復号する復号

鍵を受信する機構と、部分コンテンツに対し、復号鍵を適用する機構と、を含むものである。

【００１３】

【発明の実施の形態】以下、図面を参照して本発明のコンテンツの配信方法の実施の形態の一例を説明する。

【００１４】図１は本実施の形態におけるシステムの概略構成を示すもので、１はサーバ群、２はパーソナルコンピュータ等で構成される複数の端末、３はこれらを任意に接続するネットワークである。ここで、配信しようとする、デジタルコンテンツは、サーバ群１上に格納されているものとする。

【００１５】また、図２は前記システムにおける要部構成を示す。サーバ群１はコンテンツ要求受信手段４、コンテンツ分割手段５、復号鍵生成手段６、復号鍵提供手段７、コンテンツ暗号化手段８、コンテンツ提供手段９を備えている。また、各端末２はコンテンツ要求手段１０、復号鍵取得手段１１、コンテンツ取得手段１２、コンテンツ復号手段１３及びコンテンツ再生手段１４を備えている。なお、これらの各手段はサーバ群１及び端末２をそれぞれ構成するコンピュータとそのプログラムによって実現される。

【００１６】サーバ群１に備えられた各手段の機能と本発明の実現スキームについて説明する。

【００１７】コンテンツ要求受信手段４は端末２からのコンテンツ要求を受信する。このコンテンツ要求を受けて、端末２に対して、コンテンツ要求を受領した旨を返信するとともに、コンテンツ分割手段５が配送すべきコンテンツを任意の単位数に分割する。この分割されたコンテンツのことを以降、「分割コンテンツ」という。復号鍵生成手段６はコンテンツ分割手段５により分割された分割コンテンツ毎に復号鍵を生成する。復号鍵提供手段７は、端末２からの要求に応じて、復号鍵生成手段６により生成された復号鍵をネットワーク３を介して該端末２に提供する。

【００１８】コンテンツ暗号化手段８はコンテンツ分割手段５により分割された分割コンテンツを鍵生成手段６により生成された暗号化鍵により暗号化する。コンテンツ提供手段９はコンテンツ暗号化手段８により暗号化された分割コンテンツを端末２からの要求に応じてネットワーク３を介して該端末２に提供する。

【００１９】次に、本発明の実現スキームとサーバ群１・端末２間の通信スキームについて簡単に説明する。

【００２０】① コンテンツ要求手段１０はネットワーク３を介してサーバ群１との通信を実現し、端末２におけるユーザのコンテンツ再生命令をサーバ群１に送信する。メッセージａは再生命令に係るコンテンツを指定する情報を含む。また、これに応じて、コンテンツ要求受信手段は、要求されたコンテンツの分割情報を含むメッセージｂを返信する。ここで、コンテンツの分割情報ｂは、分割されたコンテンツを元に戻すために必要な情報

のことをいい、例えば、コンテンツ全体のサイズ、分割単位の大きさ、圧縮手法、暗号化の手法、分割されたコンテンツの順序を含む。

【００２１】② 復号鍵取得手段１１はネットワーク３を介してサーバ群１との通信を実現し、復号鍵をサーバ群１から取得する。ここで、メッセージｃは対応する鍵が必要な分割コンテンツを指定する情報を含み、メッセージｄは復号鍵を含むメッセージである。

【００２２】③ コンテンツ取得手段１２はネットワーク３を介してサーバ群１との通信を実現し、分割コンテンツをサーバ群１から取得する。ここで、メッセージｅは必要な分割コンテンツを指定する情報を含み、メッセージｆは分割コンテンツそれ自体を含むメッセージである。

【００２３】④ コンテンツ復号手段１３は、コンテンツ取得手段１２により取得した分割コンテンツを復号鍵取得手段１１により取得した復号鍵を用いて復号し、復号鍵を削除する。コンテンツ再生手段１４は、コンテンツ復号手段１３により復号された分割コンテンツの再生、削除を行う。

【００２４】以下、このスキームについて、さらに詳細な説明を加える。

【００２５】前記構成において、ユーザが端末２を利用して、特定のコンテンツの再生を命じるとコンテンツ要求手段１０が起動し、ネットワーク３を介して、前記コンテンツを指定するメッセージａをサーバ群１に送る。メッセージａを受け取ったサーバ群１は、コンテンツ要求受信手段４を起動し、コンテンツ要求受信手段４は、メッセージａからコンテンツを指定する情報を取り出す。このコンテンツ指定情報は、コンテンツ分割手段５に送られ、対応するコンテンツの分割情報を含むメッセージｂがサーバ群１からネットワーク３に返送される。コンテンツ分割手段５は、指定されたコンテンツの分割を行う。コンテンツ分割手段５は分割コンテンツをコンテンツ暗号化手段８に送るとともに、復号鍵生成手段６に暗号鍵の生成を命じる。

【００２６】復号鍵生成手段６は分割コンテンツ毎に対応する暗号鍵を生成し、生成した暗号鍵を復号鍵提供手段７及びコンテンツ暗号化手段８に送る。

【００２７】ネットワーク３を介してメッセージｂを受け取った端末２のコンテンツ要求手段１０はメッセージｂからコンテンツの分割情報を取り出し復号鍵取得手段１１に送る。

【００２８】復号鍵取得手段１１は、どの分割コンテンツに対応する鍵が必要であるかを指定するメッセージｃをネットワーク３を介して、複合鍵提供手段７に送る。ネットワーク３を介してメッセージｃを受け取ったサーバ群１の復号鍵提供手段７は、復号鍵を含むメッセージｄをネットワーク３に返送する。

【００２９】コンテンツ暗号化手段８はコンテンツ分割

手段５より受け取った分割コンテンツを復号鍵生成手段６より受け取った前記分割コンテンツに対応する暗号化鍵を使用して暗号化し、暗号化した分割コンテンツをコンテンツ提供手段９に送る。

【００３０】ネットワーク３を介してメッセージｄを受け取った端末２の復号鍵取得手段１１は復号鍵情報を取り出しコンテンツ復号手段１３に送り、コンテンツ取得手段１２に分割コンテンツの取得を命じる。

【００３１】コンテンツ取得手段１２は必要な分割コンテンツを指定するメッセージｅをネットワーク３に送る。ネットワーク３を介してメッセージｅを受け取ったサーバ群１のコンテンツ提供手段９は該当する分割コンテンツを含むメッセージｆをネットワーク３に返送する。

【００３２】ネットワーク３を介してメッセージｆを受け取った端末２のコンテンツ取得手段１２は分割コンテンツを取り出しコンテンツ復号手段１３に送る。

【００３３】コンテンツ復号手段１３はコンテンツ取得手段１２より受け取った分割コンテンツを復号鍵取得手段１１より受け取った復号鍵により復号し、コンテンツ再生手段１４に送り、復号鍵を削除する。

【００３４】コンテンツ再生手段１４はコンテンツ復号手段１３より受け取ったコンテンツを再生し削除する。

【００３５】以下同様に、コンテンツ終了まで復号鍵取得手段１１以降の手順を繰り返す。本明細書において述べた端末２に係るコンテンツ受信手段１０，複合鍵取得手段１１，コンテンツ取得手段１２，コンテンツ複合手段１３，コンテンツ再生手段１４並びにサーバ群１に係るコンテンツ要求受信手段４，コンテンツ分割手段５，複合鍵生成手段６，複合鍵提供手段７，コンテンツ暗号＊化手段８，コンテンツ提供手段９ともに、ハードウエアを用いて構成しても、ソフトウエアを用いて構成しても、あるいは、ハードウエアとソフトウエアを用いて構成してもよい。また、ネットワーク３は、公開されたインターネットに限らず、非公開のネットワークやＬＡＮ等を用いても本発明に適用することができ、さらに、有線・無線を問うものではない。

【００３６】

【発明の効果】以上説明したように、本発明によればデジタルコンテンツの配信において、正当なユーザの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる。

【００３７】また、万一の鍵が流出したとしても分割された単位コンテンツにとどまるため、コンテンツ全体を利用することはできない。よって、不正な流通、利用を効果的に防止することが可能である。

【００３８】また、サーバ群からの復号鍵の取得にあたって、ユーザ側より当該鍵の暗号化鍵をサーバ群へ送信し、サーバ群側からは当該暗号鍵で暗号化したコンテンツ復号鍵を送出することによって、ネットワーク経路上における鍵の流出を強力に防止できる。

【図面の簡単な説明】

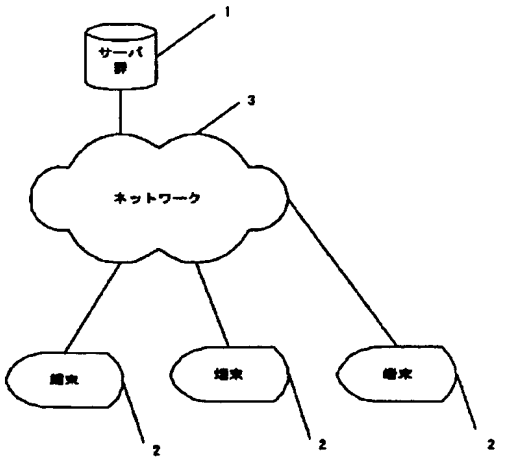
【図１】本発明が適用されるシステムを示す図である。

【図２】本発明が適用される端末とサーバ群の構成を示す図である。

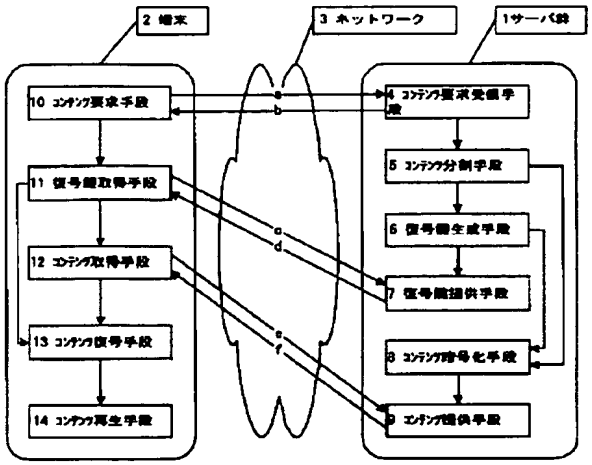
【符号の説明】

１　サーバ群
２　端末
３　ネットワーク

【図１】



【図２】



フロントページの続き

(71)出願人 501005058
中原 順志
東京都杉並区松ノ木３－33－29
(72)発明者 林 利憲
札幌市豊平区平岸１条６丁目３－56
(72)発明者 山田 康彦
東京都豊島区東池袋４丁目21－５
(72)発明者 許 先明
埼玉県所沢市寿町20－12
(72)発明者 中原 順志
東京都杉並区松ノ木３－33－29

Ｆターム(参考) 5B085 AE13 AE29 CA04
5J104 AA01 AA16 AA34 EA01 EA04
EA16 NA02 PA07